

# Managing Service Accounts for Targets using OPAM

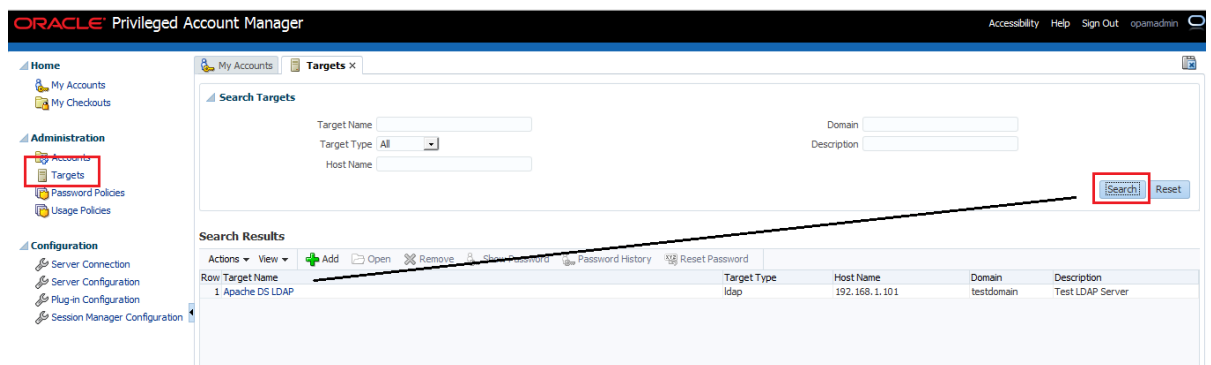
In this document, **Service Accounts** are referred to those **superuser** accounts which OPAM itself uses in order to perform its operations on the privilege accounts which it manages.

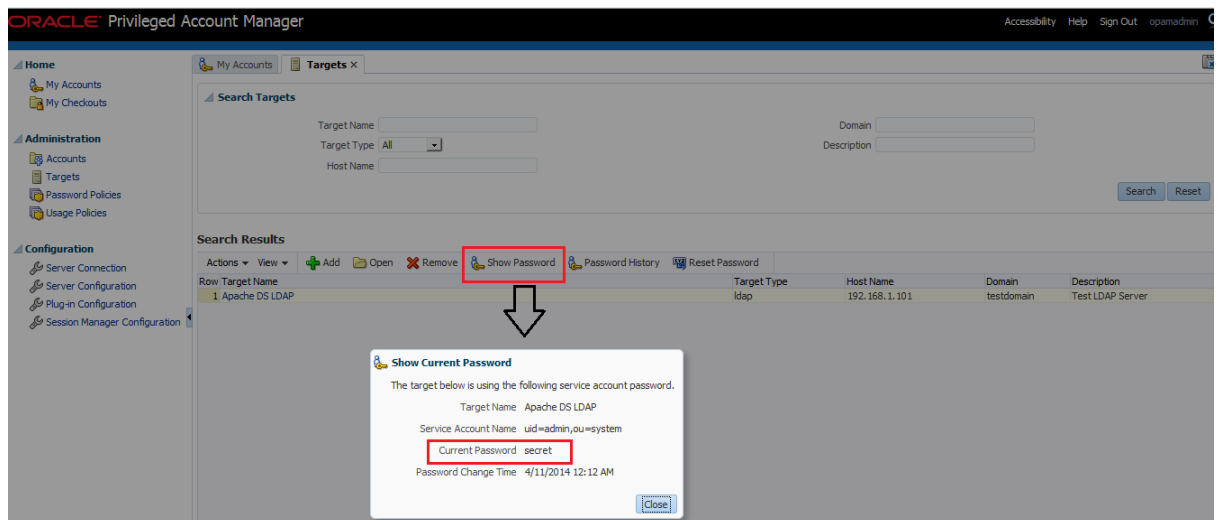
**Note:** Please do not manage the service account as a privilege account which OPAM manages. They are not the same from an OPAM context

**Pre-requisite :** The user should have Security Administrator Role.

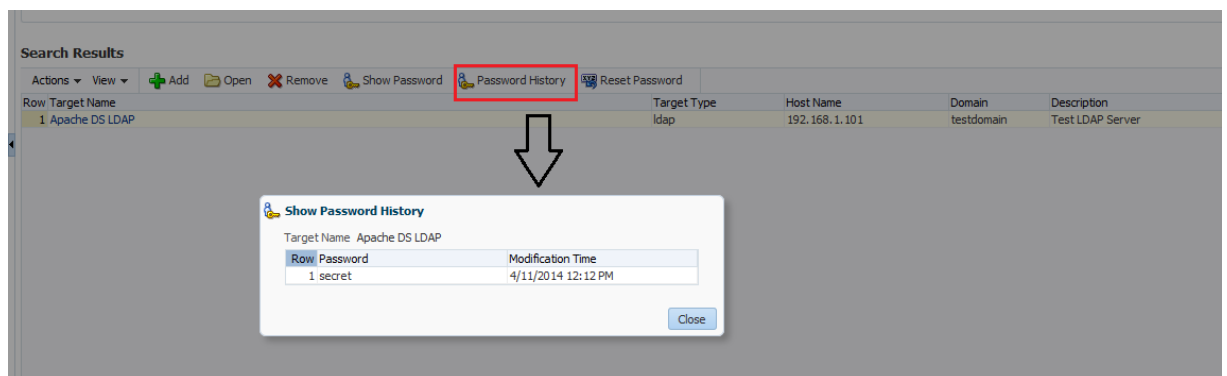
## 1. Check Service Account passwords

Log into OPAM as admin



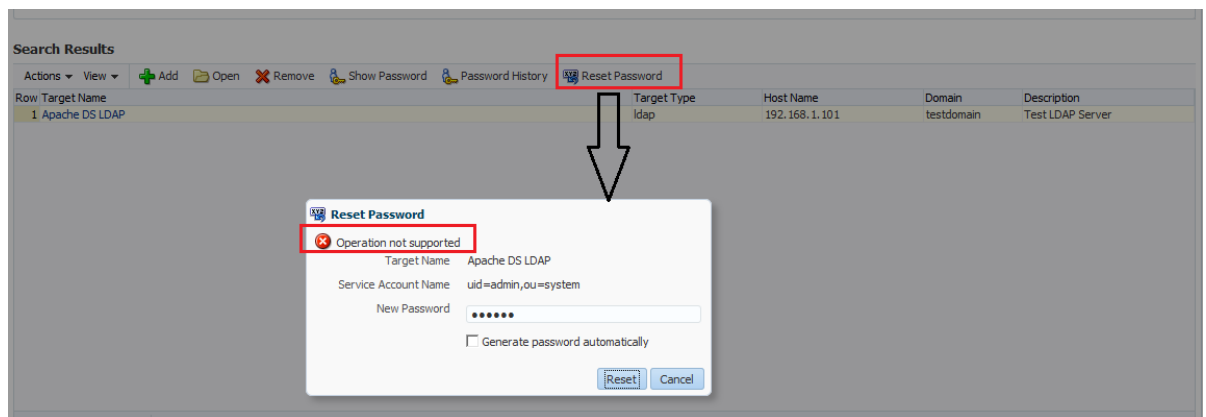


## 2. View Password History

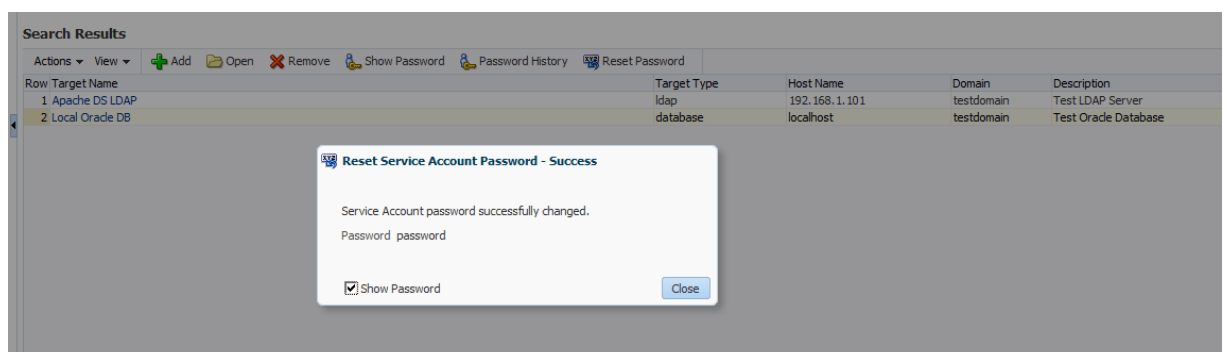
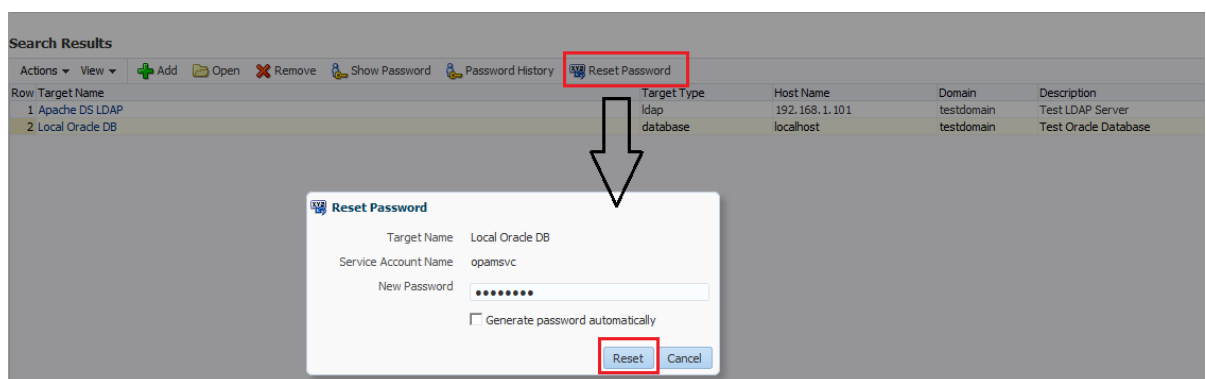


## 3. Reset Password

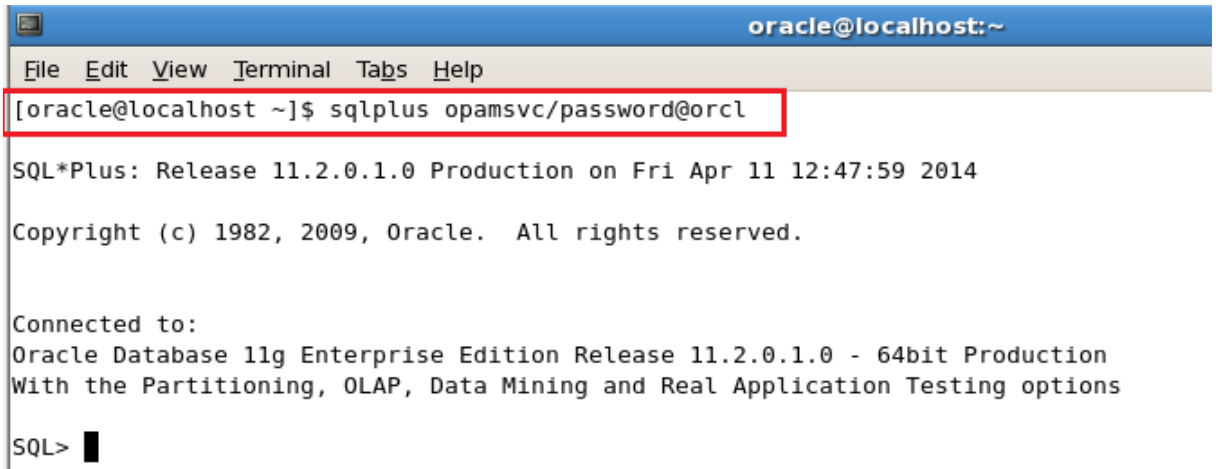
***This operation is not available for LDAP targets.***



It's available for Database targets



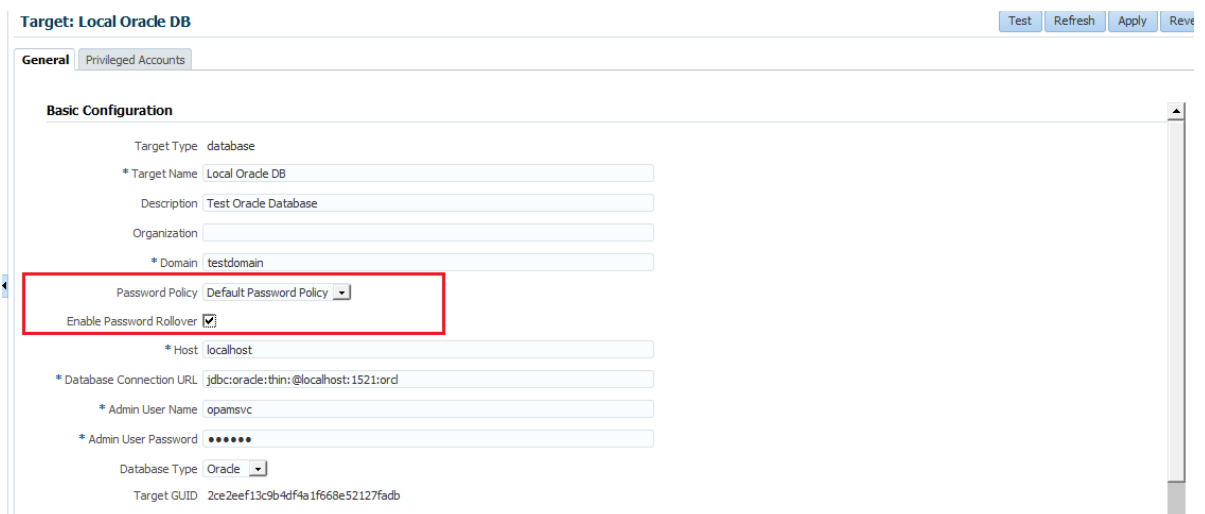
Confirm on the target system (Database)

A terminal window titled 'oracle@localhost:~' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The command '[oracle@localhost ~]\$ sqlplus opamsvc/password@orcl' is entered and highlighted with a red box. The output shows 'SQL\*Plus: Release 11.2.0.1.0 Production on Fri Apr 11 12:47:59 2014', copyright information, and connection details for 'Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production'. The prompt 'SQL>' is visible at the bottom.

```
oracle@localhost:~  
File Edit View Terminal Tabs Help  
[oracle@localhost ~]$ sqlplus opamsvc/password@orcl  
SQL*Plus: Release 11.2.0.1.0 Production on Fri Apr 11 12:47:59 2014  
Copyright (c) 1982, 2009, Oracle. All rights reserved.  
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production  
With the Partitioning, OLAP, Data Mining and Real Application Testing options  
SQL>
```

#### 4. Automatic Password management/Rollover

IF we choose Enable Rollover while creating target, ***the Password of the Service Account gets changed to a random value as per Expiration Policy*** in the Password Policy attached to the Target

A screenshot of the 'Target: Local Oracle DB' configuration page. The 'General' tab is selected. Under 'Basic Configuration', the 'Password Policy' dropdown is set to 'Default Password Policy' and 'Enable Password Rollover' is checked, both highlighted with a red box. Other fields include 'Target Name' (Local Oracle DB), 'Description' (Test Oracle Database), 'Domain' (testdomain), 'Host' (localhost), 'Database Connection URL' (jdbc:oracle:thin:@localhost:1521:ord), 'Admin User Name' (opamsvc), 'Admin User Password' (masked), 'Database Type' (Oracle), and 'Target GUID' (2ce2eef13c9b4df4a1f668e52127fadb).

Target: Local Oracle DB [Test] [Refresh] [Apply] [Revert]

General Privileged Accounts

**Basic Configuration**

Target Type: database

\* Target Name: Local Oracle DB

Description: Test Oracle Database

Organization:

\* Domain: testdomain

Password Policy: Default Password Policy

Enable Password Rollover: ☒

\* Host: localhost

\* Database Connection URL: jdbc:oracle:thin:@localhost:1521:ord

\* Admin User Name: opamsvc

\* Admin User Password: .....

Database Type: Oracle

Target GUID: 2ce2eef13c9b4df4a1f668e52127fadb

Password Policy: Default Password Policy

ApplyRevert

General

Password Complexity RulesPrivileged Accounts

General Fields

Policy Name

Default Password Policy

Policy Status

Active

Description

Default Password Policy

Password Lifecycle Rules

Save password history for

30

Days

Expire password after

20

Days

Reset password on check-in

☒

Reset password on check-out

☒